

ATTACHMENT A

**STATEMENT OF FACTS**

1. The following Statement of Facts is incorporated by reference as part of the Deferred Prosecution Agreement (the "Agreement") between the United States Department of Justice, Criminal Division, Asset Forfeiture and Money Laundering Section and the United States Attorney's Office for the Middle District of Pennsylvania (collectively, the "Department") and MoneyGram International, Inc. ("MoneyGram"). MoneyGram hereby agrees and stipulates that the following information is true and accurate. MoneyGram admits, accepts, and acknowledges that it is responsible for the acts of its officers, directors, and employees as set forth below. If this matter were to proceed to trial, the United States would prove beyond a reasonable doubt, by admissible evidence, the facts alleged below. This evidence would establish the following:
2. MoneyGram is a publicly traded, global money services business ("MSB"), incorporated under the laws of Delaware, and headquartered in Dallas, Texas. MoneyGram provides a service that enables customers to transfer money to various locations in the United States and around the world. MoneyGram operates worldwide through a network of approximately 275,000 locations in 190 countries.
3. "MoneyGram Outlets" or "Outlets" are independently owned entities that are contractually authorized to transfer money through MoneyGram's money transfer system. Typically, MoneyGram Outlets are businesses that primarily provide other types of goods and services, and also offer money transfers through MoneyGram.
4. "MoneyGram Agents" or "Agents" are individuals or entities that own and/or operate MoneyGram Outlets. MoneyGram Agents receive a commission from MoneyGram on transactions processed at their Outlets. MoneyGram Agents are independent contractors, not MoneyGram employees. MoneyGram has the legal right to terminate an Agent for a variety of reasons, including suspected involvement in fraud or money laundering.
5. "Perpetrators" were individuals that created schemes to defraud the public using MoneyGram's money transfer system. These Perpetrators included, among other people, certain MoneyGram Agents.
6. The "MoneyGram Call Center" or "Call Center" is located in or around Lakewood, Colorado. Among other responsibilities, the Call Center fields complaints of MoneyGram customers from around the world who report they were the victims of fraud. These complaints, known as "Consumer Fraud Reports," are typically filed by the customer within a few days of the fraudulent transaction. The Consumer Fraud Report lists the name and address of the customer who was allegedly victimized, the send amount, the date of the transfer, the intended recipient, and a description from the customer of how they believe they were defrauded. The Call Center then forwards the Consumer Fraud Report data to MoneyGram's Fraud Department for investigation.

**FILED  
HARRISBURG**

**NOV 9 - 2012**

**MARY E. D'ANDREA, CLERK**  
Per \_\_\_\_\_  
**DEPUTY CLERK**

MoneyGram's Money Transfer System

7. To send money using MoneyGram's money transfer system, customers go to a MoneyGram Outlet and complete a "send" form designating the name of the recipient and the state or province and country where the money is to be sent. The MoneyGram Agent is required to enter the information from the send form along with the transfer amount into a transaction database established and maintained by MoneyGram as part of its central electronic network in or around Minneapolis, Minnesota. MoneyGram charges a fee based on the transfer amount and the destination location. Customers then give the MoneyGram Agent cash to cover the transfer amount and the MoneyGram fee. Customers are given an eight-digit MoneyGram reference number for the transaction.
8. To receive a money transfer, MoneyGram requires the payee to physically appear at a MoneyGram Outlet and complete a handwritten application known as a "receive" form. On the receive form, MoneyGram requires the payee to list his or her name, address and telephone number; the name, city, state or province of the sender; and the expected transfer amount. The MoneyGram Agent then queries MoneyGram's transaction database to find the money transfer intended for the payee. For all money transfers in amounts equal to or greater than \$900, MoneyGram requires the payee to present a valid identification document for examination by the MoneyGram Agent. MoneyGram then requires the MoneyGram Agent to enter the payee's name, address, telephone number, and identification document serial number into its transaction database. Depending on the MoneyGram Outlet, the payee will receive the money in cash or in the form of a MoneyGram transfer check or money order.
9. Money transferred between two individuals using MoneyGram's money transfer system is never actually physically transported from the sender to the receiver. Rather, the details from the send transaction are recorded in MoneyGram's transaction database. The sending Agent is then responsible for depositing the cash it received from the customer into its bank account by the next business day. MoneyGram then removes the transfer amount plus the MoneyGram fee from the Agent's bank account typically on the second business day after the transaction. Even though the customer's money does not reach MoneyGram's account for at least two business days, MoneyGram makes the funds available to the payee as soon as ten minutes after the initial transaction based on the information it has in its transaction database. Depending on the contractual agreement between the payout Agent and MoneyGram, the Agent pays the payee with cash on hand or issues the payee a MoneyGram transfer check or money order. MoneyGram then adds money to the payout Agent's bank account for the money paid to the payee. At all times before the payee receives cash from the MoneyGram Agent or cashes the MoneyGram transfer check, MoneyGram has the ability to refuse to conduct a transaction, reverse a transaction, or stop payment on the MoneyGram transfer check at its discretion.

The Fraud Scheme Operated through MoneyGram's Money Transfer System

10. From as early as 2003, and continuing into 2009, MoneyGram, through the Consumer Fraud Reports and other data its Fraud Department collected, knew that specific MoneyGram Agents were involved in a fraud scheme that relied on a variety of false promises and other

representations to the public in order to trick unsuspecting victims into sending money through participating MoneyGram Agents and MoneyGram Outlets. The victims' money would then be taken by the Perpetrators and none of the false promises or representations were fulfilled. Specifically, victims were contacted by phone, U.S. mail, interstate courier, or the Internet, and were fraudulently induced to send money to the Perpetrators. The fraud was committed by, among other things:

- a. Falsely promising victims they would receive large cash prizes, lottery winnings, fictitious loans, or other payments;
  - b. Falsely offering various high-ticket items for sale over the Internet at deeply discounted prices;
  - c. Falsely promising employment opportunities as "secret shoppers" who would be paid to evaluate retail stores; or
  - d. Placing a distressed phone call falsely posing as the victim's relative and claiming to be in trouble and in urgent need of money.
11. The Perpetrators then falsely represented that in order to receive the item the victims were promised, the victims needed to give the Perpetrators some money in advance. For example, in situations where the victims were promised cash prizes or lottery winnings, the victims were told they had to pay taxes, customs' duties, or processing fees up front. The victims were then directed to send the advance payments to fictitious payees using MoneyGram's money transfer system.
12. After the victims completed the money transfer, they were instructed to contact the Perpetrators to give them the MoneyGram reference number for the transaction. The Perpetrators then brought the victims' MoneyGram reference number to participating MoneyGram Agents to remove the victims' money from the MoneyGram money transfer system.
13. The MoneyGram Agents knowingly entered false addresses, telephone numbers, and personal identification document information for these transactions into the MoneyGram database. In doing so, the MoneyGram Agents concealed the true identities of the Perpetrators, as well as their ownership and control of the fraudulently obtained funds. The MoneyGram Agents then gave the Perpetrators the victims' money, after subtracting their own fees for completing the fraudulent transaction.
14. At no time were the victims provided with what they were falsely promised by the Perpetrators.

MoneyGram Knew Its Agents Were Involved in the Fraud Scheme

15. From in or about 2004 through 2009, MoneyGram customers filed approximately 63,814 Consumer Fraud Reports involving transfers paid out at MoneyGram Outlets in the United States and Canada totaling approximately \$128,445,411 in losses to victims. The victims who generated the vast majority of these Consumer Fraud Reports described losing money through the scheme outlined above. The total scope of the fraud scheme, however, is more expansive because not every victim of the fraud scheme reported the fraud to MoneyGram.
16. As early as 2003, MoneyGram's Fraud Department was compiling the Consumer Fraud Report data in an electronic fraud database that detailed the number of fraud complaints for each MoneyGram Agent. Within MoneyGram, the Fraud Department recommended to senior management that numerous specific MoneyGram Agents and Outlets be terminated for fraud due to the high number of Consumer Fraud Reports generated.
17. Despite these recommendations, MoneyGram's former senior management refused to allow its Fraud Department to terminate an Agent or close an Outlet for fraud without approval from executives on the sales side of the business. As a result, the Fraud Department's termination recommendations were rarely accepted. For example, in March 2007, the Fraud Department – after receiving a Civil Investigative Demand from the Federal Trade Commission regarding consumer fraud in Canada – recommended that MoneyGram immediately close 32 specific MoneyGram Outlets in Canada that had high levels of reported fraud. These Outlets were described by MoneyGram's Senior Director of Anti-Money Laundering as "the worst of the worst" and "beyond anyone's ability to doubt that the agent had knowledge and involvement." On April 20, 2007, a meeting was held to discuss the closure of these Outlets. In attendance at the meeting were MoneyGram officers at the senior and executive vice-president level. Ultimately, these officers rejected the Fraud Department's recommendation and did not close any of the 32 Outlets. Following this decision, MoneyGram continued to receive complaints from its customers indicating these MoneyGram Outlets were still involved in fraud. Nevertheless, MoneyGram continued to process transactions from the Outlets that they knew were involved in fraud.

MoneyGram Assisted and Profited from the Fraud Scheme

18. Despite its knowing that specific MoneyGram Agents were involved in the fraud scheme, MoneyGram continued to process fraudulent transactions through these Agents. MoneyGram's processing of these fraudulent transactions was critical to the success of the fraud scheme because the Perpetrators relied on MoneyGram's money transfer system to receive the victims' money.
19. MoneyGram's Fraud Department attempted to implement policies that would require the termination of a MoneyGram Agent or Outlet if the Agent or Outlet had a certain number of Consumer Fraud Reports. These policies were repeatedly rejected by the sales side of the business. For example, in March 2007, MoneyGram's Fraud Department recommended that MoneyGram terminate any Agent that had 15 Consumer Fraud Reports in three months, 20 Consumer Fraud Reports in six months, or 40 Consumer Fraud Reports in one year. This policy was never approved by sales and therefore never implemented.

20. Subsequently, in or about November 2008, sales finally approved a termination policy. Under the approved policy, MoneyGram would terminate any Agent that had Consumer Fraud Reports greater than one percent of all MoneyGram's Consumer Fraud Reports *worldwide*. In 2008, there were approximately 27,000 Consumer Fraud Reports filed worldwide. Thus, MoneyGram's policy meant an Agent would not be terminated for fraud unless the Agent incurred at least 270 Consumer Fraud Reports in one year – nearly seven times as many Consumer Fraud Reports as under the March 2007 proposed policy. Even this weaker policy was never consistently enforced prior to April 2009.
21. As a result of MoneyGram's failure to implement a termination policy, MoneyGram Agents complicit in the fraud were permitted to stay open for longer periods of time and the fraudulent activity skyrocketed. In 2004, victimized MoneyGram customers in the United States and Canada filed approximately 1,575 Consumer Fraud Reports. For 2008, that number jumped over ten fold, to approximately 19,614 reported frauds.
22. MoneyGram also actively assisted certain Agents engaged in fraud by increasing the number of transactions these Agents could process each day, granting these Agents additional MoneyGram Outlets from which to operate, and increasing their compensation.
23. One example was MoneyGram Agent James Ugoh. Ugoh came to own and/or control 12 MoneyGram outlets in Toronto, Canada. For years, Ugoh's Outlets were recognized by MoneyGram's Fraud Department as some of MoneyGram's top fraud Outlets. The following timeline details Ugoh's relationship with MoneyGram:
 

Dec. 2001	Ugoh becomes a MoneyGram Agent and opens an Outlet called "Money Spot."
Aug. 2004	MoneyGram's Manager of the Fraud and Compliance Departments recognizes that Ugoh's Money Spot has an "unusually high" number of fraud complaints. Nevertheless, that same month, MoneyGram authorizes Ugoh to open two additional outlets, "Money Spot 2" and "Money Spot 3."
Mar. 2005	MoneyGram authorizes Ugoh to open another outlet, "Money Spot 4." By this time, there have been 66 Consumer Fraud Reports filed that involve Ugoh's other Outlets, totaling \$250,463 in losses to victims.
June 2005	MoneyGram sponsors a party in Ugoh's honor in recognition of his work for MoneyGram. The MoneyGram name is on the invitation. At this point, 96 Consumer Fraud Reports have been filed totaling \$348,310 in losses to victims.
Feb. 2006	MoneyGram's Fraud Department identifies Money Spot, Money Spot 2, and N&E Associates (run by Ugoh but in his wife's name) as leading fraud Outlets.

June 2006	MoneyGram authorizes Ugoh to open "Money Spot 5." At this point, 284 Consumer Fraud Reports have been filed totaling \$785,791 in losses to victims.
July 2006	MoneyGram restricts Money Spot's ability to receive transactions because of fraud. The restriction is lifted after intervention from the sales side of the business.
Aug. 2006	MoneyGram authorizes Ugoh to open "Money Spot 6." At this point, 343 Consumer Fraud Reports have been filed totaling \$904,286 in losses to victims.
Sept. 2006	MoneyGram pays Ugoh a \$70,000 "re-signing bonus."
Jan. 2007	MoneyGram's Fraud and Anti-Money Laundering Departments identify that Money Spot is working with other MoneyGram Agents to launder fraud proceeds using MoneyGram transfer checks.
Mar. 2007	MoneyGram authorizes Ugoh to open "Money Spot 7" and "Money Spot 8." At this point, 544 Consumer Fraud Reports have been filed totaling \$1,304,521 in losses to victims.
Apr. 2007	MoneyGram's Fraud Department recommends the immediate closure of Money Spot, Money Spot 2, and N&E Associates as part of a larger proposal to terminate 32 of its worst high-fraud Canadian Outlets. MoneyGram senior executives reject the recommendation and allow all of Ugoh's Outlets to remain open.
June 2007	MoneyGram authorizes Ugoh to open "Money Spot 9" and "Money Spot 10." At this point, 665 Consumer Fraud Reports have been filed totaling \$1,542,818 in losses to victims.
July 2007	MoneyGram awards Money Spot the status of "Red Store," a corporate marketing reward for its top performing Outlets. That same month, MoneyGram's internal Fraud Report lists Money Spot as its top fraud Outlet.
Aug. 2007	MoneyGram increases Ugoh's commission. MoneyGram makes the commission increase retroactive to September 2006.
Dec. 2007	Money Spot is number one again on MoneyGram's internal Fraud Report. Money Spot 2, Money Spot 4, and N&E Associates are all in the top nine for fraud in Ontario.
Mar. 2008	MoneyGram authorizes Ugoh to open "Money Spot 11." At this point, 1,130 Consumer Fraud Reports have been filed totaling \$2,384,263 in losses to victims.
July 2008	MoneyGram's Fraud Department recognizes that all 12 Outlets owned or controlled by Ugoh have received fraudulent transactions.

Feb. 2009 All Money Spot Outlets are closed incident to Toronto Police Department's execution of search warrants at various MoneyGram Outlets.

By the time Ugoh's Outlets were closed, MoneyGram had received 1,733 Consumer Fraud Reports totaling over \$3.3 million in losses to victims. These Consumer Fraud Reports, however, are just the tip of the iceberg. From January 2005 through February 2009, Ugoh's Outlets received over \$27.8 million from the United States. According to Ugoh, nearly all of the money received at his Outlets from the United States was fraud proceeds.

24. From 2004 to 2009, MoneyGram had 264 Agents in the United States and Canada with over 50 Consumer Fraud Reports. The reported fraud from these Agents alone represents over \$75,000,000 in losses to victims.
25. MoneyGram profited from the fraud scheme by, among other ways, collecting fees and other revenues on each fraudulent transaction initiated by the Perpetrators including MoneyGram Agents.

#### Laundering of Fraud Proceeds Using MoneyGram's Money Transfer System

##### Toronto Money Laundering Scheme

26. Beginning in 2006 and continuing into early 2009, Ugoh conspired with at least 25 corrupt MoneyGram Agents in the Toronto area in a large-scale money laundering scheme designed to conceal where the proceeds from the fraud scheme were being sent. Complicit MoneyGram Agents in Canada received the initial fraudulent transaction from the victim via the MoneyGram money transfer system. The complicit MoneyGram Agents then executed their money laundering scheme by making the MoneyGram transfer check payable to one of a few individuals responsible for laundering the money ("laundering Agents") instead of to a fictitious payee to whom the victims believed the money was being sent. The checks were then collected and deposited into business accounts controlled by the laundering Agents. This practice, known as "check pooling," allowed Ugoh and others to collect MoneyGram transfer checks from multiple Outlets, deposit the checks into what otherwise appeared to be legitimate bank accounts, and then ultimately withdraw and distribute the proceeds among the Perpetrators.
27. MoneyGram's Fraud and Anti-Money Laundering Departments were aware of this scheme as early as January 2007, when an employee in MoneyGram's Agent Services Department sent an e-mail to numerous people in the Fraud and Anti-Money Laundering Departments describing the scheme. The e-mail specifically noted MoneyGram transfer checks used in transactions reported as fraud were made out to Ugoh's Money Spot and another MoneyGram Outlet called "Modicom Accounting" instead of the purported payee. Before sending the e-mail, the Agent Services employee contacted the bank where the checks representing the fraud proceeds were being deposited. The bank offered to call MoneyGram each time there was an attempt to deposit one of these checks so that MoneyGram could stop payment. The Agent Services employee ended the e-mail pleading that "there has to be something we could do about this[,] we have to try as hard as we can to make this stop." Despite this, MoneyGram did nothing to investigate or stop the activity. MoneyGram did not

investigate or terminate the Agents involved and did not take up the bank's offer to stop payment on the checks. As a result, the activity continued unabated into 2009.

U.S. Agents Money Laundering

28. As early as 2006 and continuing into 2009, complicit MoneyGram Agents in the United States conspired with MoneyGram Agents throughout the world to launder fraud proceeds using the MoneyGram money transfer system. In these schemes, complicit Agents in the United States would receive the initial fraudulent transaction from the victim via the MoneyGram money transfer system. Then after taking a commission, the complicit Agent in the United States would use the MoneyGram money transfer system to send the remaining money to complicit MoneyGram Agents around the world. This two-step process was designed to conceal the ultimate destination of the fraud proceeds. Despite identifying certain Agents involved in this activity as early as 2007, MoneyGram allowed the Agents to remain open and the activity continued into 2009.

MoneyGram Willfully Failed to Maintain an Effective Anti-Money Laundering Program

29. Congress enacted the Bank Secrecy Act, Title 31, United States Code, Sections 5311 *et seq.* ("BSA"), and its implementing regulations to address an increase in criminal money laundering activity utilizing financial institutions. Among other provisions, it requires MSBs like MoneyGram to maintain programs designed to detect and report suspicious activity that might be indicative of money laundering, terrorist financing, and other financial crimes, and to maintain certain records and file reports related thereto that are especially useful in criminal, tax, or regulatory investigations or proceedings.
30. Pursuant to 31 U.S.C. § 5318(h) and 31 C.F.R. § 103.125 (now renumbered 31 C.F.R. § 1022.210), MoneyGram was required to establish and maintain an anti-money laundering ("AML") compliance program that, at a minimum:
- a. provides internal policies, procedures, and controls designed to guard against money laundering;
  - b. provides for an individual or individuals to coordinate and monitor day-to-day compliance with the BSA and AML requirements;
  - c. provides for an ongoing employee training program; and
  - d. provides for independent testing for compliance by bank personnel or an outside party.
31. In the Middle District of Pennsylvania and elsewhere, MoneyGram willfully failed to maintain an effective anti-money laundering program that was reasonably designed to prevent it from being used to facilitate money laundering. These failures included, among others:

- a. MoneyGram failed to implement policies or procedures governing the termination of Agents involved in fraud and money laundering.
- b. MoneyGram filed Suspicious Activity Reports ("SARs"), in which MoneyGram incorrectly listed the victim of the fraud as the individual who was the likely wrongdoer. MoneyGram failed to file SARs on their Agents who MoneyGram knew were involved in the fraud.
- c. MoneyGram failed to implement policies or procedures to file the required SARs when victims reported fraud to MoneyGram on transactions over \$2,000. Instead, MoneyGram structured its AML program so that individuals responsible for filing SARs did not have access to the Fraud Department's Consumer Fraud Report database.
- d. MoneyGram failed to sufficiently resource and staff its AML program.
- e. MoneyGram failed to conduct effective AML audits of its Agents and Outlets. MoneyGram's Senior Director of Anti-Money Laundering refused to conduct audits on certain Outlets involved in fraud and money laundering that MoneyGram refused to terminate because the Outlets were "criminal operations" and sending their audit team in to those Outlets would put the audit team in "physical danger."
- f. MoneyGram failed to implement policies or procedures to review MoneyGram transfer checks of Agents known or suspected to be involved in "check pooling." As described above, MoneyGram knew its Agents were using MoneyGram transfer checks to launder fraud proceeds and did nothing to investigate the activity or prevent it from occurring in the future.
- g. MoneyGram failed to conduct adequate due diligence on prospective MoneyGram Agents. MoneyGram routinely signed up new Agents without visiting the locations or verifying that a legitimate business existed. As a result, some of the Agents involved in fraud and money laundering operated out of homes in residential neighborhoods and other locations that were not open to the public.
- h. MoneyGram failed to conduct adequate due diligence on MoneyGram Agents seeking additional MoneyGram Outlets. MoneyGram routinely granted additional Outlets to Agents known to be involved in fraud and money laundering.

#### MoneyGram's Remedial Actions

32. Beginning in 2009, MoneyGram began taking remedial actions to address shortcomings in its anti-fraud and anti-money laundering programs. These remedial measures include:
- a. In March and April 2009, MoneyGram closed over 250 Outlets believed to be involved in consumer fraud at the request of the U.S. Attorney's Office for the Middle District of Pennsylvania. Within six months, MoneyGram closed over 150 additional Agents determined to be involved in consumer fraud.

- b. The entire senior management team in place prior to April 2009 has been replaced.
- c. MoneyGram has increased the number of employees in the Compliance Department by nearly 100%. This includes an approximate fivefold increase in staffing in the Fraud Department.
- d. MoneyGram has created two new executive level positions: (1) Senior VP, Global Security and Investigations – responsible for enhancing efforts to combat consumer fraud and fostering cooperation with law enforcement; (2) Senior VP, Associate General Counsel Global Regulatory and Chief Privacy Officer – responsible for enhancing interaction with U.S. and International regulators and enhancing MoneyGram's compliance systems.
- e. MoneyGram has created a Financial Intelligence Unit within the Compliance Department which includes a manager and thirteen analysts. The Financial Intelligence Unit monitors Agent behavior, analyzes high risk transactions, conducts reviews of Agents, and files specialized SARs for Agents.
- f. MoneyGram created an Anti-Fraud Alert System. The system identifies and then places on hold potentially fraudulent transactions. MoneyGram then contacts the sender to determine the legitimacy of the transactions. If MoneyGram believes the transaction is the result of fraud the transaction is cancelled and the money returned to the sender. MoneyGram has 17 full time employees dedicated to the system and has to date prevented over one hundred million dollars in consumer fraud transactions.
- g. MoneyGram has strengthened its Agent termination policy and now terminates any Agent believed to be involved in any way with illegal activity.
- h. MoneyGram's Fraud and AML Departments now share information. As a result, MoneyGram now files SARs on Agents involved in fraud and money laundering and on all transactions over \$2,000 that are reported as fraud.
- i. MoneyGram has implemented a risk-based Agent audit program that takes into account an Agent's location and number of Consumer Fraud Reports.
- j. MoneyGram has implemented a new Agent training program that provides information on the types of consumer fraud scams as well as how to detect, prevent, report and handle suspicious transactions.

ATTACHMENT B

**CERTIFICATE OF CORPORATE RESOLUTIONS**

WHEREAS, MONEYGRAM INTERNATIONAL, INC. (the "Company") has been engaged in discussions with the United States Department of Justice, Criminal Division, Asset Forfeiture and Money Laundering Section and the United States Attorney's Office for the Middle District of Pennsylvania (collectively, the "Department") regarding fraud-induced money transfers, money laundering, and the Company's anti-money laundering program; and

WHEREAS, in order to resolve such discussions, it is proposed that the Company enter into a certain agreement with the Department; and

WHEREAS, the Company's Executive Vice President, General Counsel and Corporate Secretary, Francis Aaron Henry, together with outside counsel for the Company, have advised the Board of Directors of the Company of its rights, possible defenses, the Sentencing Guidelines' provisions, and the consequences of entering into such agreement with the Department;

Therefore, the Board of Directors has RESOLVED that:

1. The Company (a) acknowledges the filing of the two-count Information charging the Company with aiding and abetting wire fraud, in violation of Title 18, United States Code, Sections 1343 and 2, and willfully failing to implement an effective anti-money laundering program, in violation of Title 31, United States Code, Section 5318(h) and regulations issued thereunder; (b) waives indictment on such charges and enters into a deferred prosecution agreement with the Department; and (c) agrees to forfeit \$100,000,000 to the United States;

2. The Chairman and Chief Executive Officer, Pamela H. Patsley, is hereby authorized, empowered and directed, on behalf of the Company, to execute the Deferred


Prosecution Agreement substantially in such form as reviewed by this Board of Directors at this meeting with such changes as the Chairman and Chief Executive Officer, Pamela H. Patsley, may approve;

3. The Chairman and Chief Executive Officer, Pamela H. Patsley, is hereby authorized, empowered and directed to take any and all actions as may be necessary or appropriate and to approve the forms, terms or provisions of any agreement or other documents as may be necessary or appropriate, to carry out and effectuate the purpose and intent of the foregoing resolutions; and

4. All of the actions of the Chairman and Chief Executive Officer, Pamela H. Patsley, which actions would have been authorized by the foregoing resolutions except that such actions were taken prior to the adoption of such resolutions, are hereby severally ratified, confirmed, approved, and adopted as actions on behalf of the Company.

Date: November 8, 2012

By:

  
Francis Aaron Henry  
Executive Vice President, General Counsel  
and Corporate Secretary  
MoneyGram International, Inc.

ATTACHMENT C

**ENHANCED COMPLIANCE UNDERTAKING**

In addition to the enhancements MoneyGram International, Inc. (the "Company") has already made to its anti-fraud and anti-money laundering programs as described in the Statement of Facts and the Mandate of the Corporate Compliance Monitor discussed in Attachment D, the Company agrees that it has or will undertake the following:

*Board of Directors*

1. The Company will create an independent Compliance and Ethics Committee of the Board of Directors with direct oversight of the Chief Compliance Officer and the Compliance Program. This Committee will be responsible for ensuring that the Company is in compliance with all aspects of this Agreement. All reports submitted as a part of this Agreement shall be sent under the cover of this Committee.

*Adopt a Worldwide Anti-Fraud and Anti-Money Laundering Standard*

2. The Company will require all MoneyGram Agents around the world, regardless of their location, to adhere to either the anti-fraud and anti-money laundering standards as defined by the FATF interpretive guidelines for Money Services Businesses or the U.S. anti-fraud and anti-money laundering standards, whichever is stricter. This new policy will ensure that all MoneyGram Agents throughout the world will, at a minimum, be required to adhere to U.S. anti-fraud and anti-money laundering standards.
3. The Company will design and implement a risk-based program to audit MoneyGram Agents throughout the world to ensure they are complying with the new policy referenced in paragraph 2 of this attachment.

*Executive Review and Bonus Structure*

4. The Company will restructure its executive review and bonus system so that each MoneyGram executive is evaluated on what they have done to ensure that their business or department adheres to international compliance-related policies and procedures and related U.S. regulations and laws. A failing score in compliance will make the executive ineligible for any bonus for that year.
5. The Company will include in its new executive review and bonus system a provision that allows the Company to "claw back" prior bonuses for executives later determined to have contributed to compliance failures.

*Agent Due Diligence Remediation*

6. The Company will design and implement a remediation plan to review the due diligence, selection, and retention files for all MoneyGram Agents worldwide with more than one (1) complaint in any rolling thirty (30) day period, beginning in 2009, from consumers alleging transactions paid at any one of the Agent's Outlets were the result of fraud. This remediation plan should ensure that MoneyGram has done the proper due diligence on each of these Agents.
7. On Agents deemed by MoneyGram to be high risk or operating in a high risk area, MoneyGram will develop and implement a plan to conduct enhanced due diligence.

*Anti-Fraud Alert System*

8. The Company will ensure, as directed by the Monitor, that the maximum number of transactions feasible, originating in the United States, regardless of the destination, will

be reviewed in the Company's Anti-Fraud Alert System to identify potentially fraudulent transactions.

*Transaction Monitoring*

9. The Company will develop and implement a risk-based program, using the best tools available, to test and verify the accuracy of the sender and receiver biographical and identification data entered into the transaction database by MoneyGram Agents.

*Suspicious Activity Reports*

10. The Company will follow all laws and regulations concerning the filing of Suspicious Activity Reports ("SARs") in the United States for any suspicious activity, as defined by the Bank Secrecy Act and its implementing regulations, including suspicious activity identified by the Company that originates in the United States, regardless of where in the world the suspicious transactions is received.

*High Risk Countries*

11. The Company will assign at least one Anti-Money Laundering Compliance Officer to oversee compliance for each country that the Company has designated as high risk for fraud or money laundering. By developing an expertise in their assigned high risk country, the Compliance Officer will better enable the Company to detect and prevent fraud and money laundering activities in those countries.

*Reporting requirements*

12. The Company will provide the Department with a report every ninety (90) days listing:
  - (1) all MoneyGram Outlets worldwide with ten (10) or more complaints from consumers

during the previous twelve (12) months alleging transactions paid at the Outlet were the result of fraud; (2) for each Outlet on the list, the Company will identify the owner of the Outlet, total fraud complaints since the Outlet opened, total number of receives for the prior year, total dollar value of the receives for the prior year, the average dollar value for receive transactions, total number of sends for the prior year, total dollar value of the sends for the prior year, the average dollar value for send transactions, total revenue earned by MoneyGram from the Outlet for the prior year (including, but not limited to, transfer fees and currency exchange revenue), any additional Outlets with the same owner, and the total consumer fraud complaints for each other Outlet with the same owner; (3) for each Outlet on the list, the Company will describe what actions, if any, have been taken against the Outlet and/or Agent and describe why such action (or lack of action) was deemed appropriate.

13. The Company will provide the Department with a report every ninety (90) days of all MoneyGram Agents or Outlets worldwide that were terminated, suspended or restricted in any way during the previous ninety (90) days based on fraud or money laundering concerns and whether or not a SAR was filed.
14. The Company will provide the Department with a report every ninety (90) days listing all termination, suspension or restriction recommendations during the previous ninety (90) days by the Company's Fraud, Anti-Money Laundering or Compliance Departments that were not accepted and an explanation of why. The Company should also indicate whether or not a SAR was filed.

15. The Company will, on a monthly basis, submit electronically to the Federal Trade Commission ("FTC"), or its designated agent, for inclusion in the Consumer Sentinel Network, a secure online database operated by the FTC and available to law enforcement, all relevant information the Company possesses in its consumer fraud database, for Agents and Outlets worldwide, regarding consumer complaints about alleged fraud-induced money transfers and regarding the underlying transfers themselves, including but not limited to, the name and address of the sender, the send location, the date and amount of the transfer, the transfer fee, the date and actual location of the receipt, the name of the receiver, any information regarding the receiver's identification, the reference number for the transfer, the nature of the consumer's complaint, and any additional details provided by the consumer. Provided, however, that the Company may decline to provide this information if it receives a request from a consumer that is documented by the Company stating that he or she does not want the information to be shared with law enforcement.

ATTACHMENT D

**CORPORATE COMPLIANCE MONITOR**

The duties and authority of the Corporate Compliance Monitor (the "Monitor"), and the obligations of MoneyGram International, Inc. (the "Company"), with respect to the Monitor and the Department, are as described below:

1. The Monitor will for a period of up to five (5) years from the date of his engagement (the "Term of the Monitorship") evaluate, in the manner set forth in Paragraphs 2 through 8 below, the effectiveness of the internal controls, policies and procedures of the Company's anti-fraud and anti-money laundering programs, the Company's overall compliance with the Bank Secrecy Act, the Company's maintenance of the remedial measures enumerated in the Statement of Facts, as well as the Company's implementation of the Enhanced Compliance Undertaking discussed in Attachment C, and take such reasonable steps as, in his or her view, may be necessary to fulfill the foregoing mandate (the "Mandate").

2. The Company shall cooperate fully with the Monitor and the Monitor shall have the authority to take such reasonable steps as, in his view, may be necessary to be fully informed about the Company's compliance program within the scope of the Mandate in accordance with the principles set forth herein and applicable law, including applicable data protection and labor laws and regulations. To that end, the Company shall: (a) facilitate the Monitor's access to the Company's documents and resources, (b) not limit such access, except as provided in this paragraph, and (c) provide guidance on applicable local law (such as relevant data protection and labor law). The Company shall provide the Monitor with access to all information, documents, records, facilities and/or employees, as reasonably requested by the Monitor, that fall within the scope of the Mandate of the Monitor under this Agreement. Any disclosure by the Company to

the Monitor concerning fraud-induced money transfers, money laundering, or its anti-money laundering program shall not relieve the Company of any otherwise applicable obligation to truthfully disclose such matters to the Department.

a. The parties agree that no attorney-client relationship shall be formed between the Company and the Monitor.

b. In the event that the Company seeks to withhold from the Monitor access to information, documents, records, facilities and/or employees of the Company which may be subject to a claim of attorney-client privilege or to the attorney work-product doctrine, or where the Company reasonably believes production would otherwise be inconsistent with applicable law, the Company shall work cooperatively with the Monitor to resolve the matter to the satisfaction of the Monitor. If the matter cannot be resolved, at the request of the Monitor, the Company shall promptly provide written notice to the Monitor and the Department. Such notice shall include a general description of the nature of the information, documents, records, facilities and/or employees that are being withheld, as well as the basis for the claim. The Department may then consider whether to make a further request for access to such information, documents, records, facilities and/or employees. To the extent the Company has provided information to the Department in the course of the investigation leading to this action pursuant to a non-waiver of privilege agreement, the Company and the Monitor may agree to production of such information to the Monitor pursuant to a similar non-waiver agreement.

3. To carry out the Mandate, during the Term of the Monitorship, the Monitor shall conduct an initial review and prepare an initial report, followed by at least four (4) follow-up reviews and reports as described below. With respect to each review, after meeting and consultation with the Company and the Department, the Monitor shall prepare a written work

plan, which shall be submitted no fewer than sixty (60) calendar days prior to commencing each review to the Company and the Department for comment, which comment shall be provided no more than thirty (30) calendar days after receipt of the written work plan. The Monitor's work plan for the initial review shall include such steps as are reasonably necessary to conduct an effective initial review in accordance with the Mandate, including by developing an understanding, to the extent the Monitor deems appropriate, of the facts and circumstances surrounding any violations that may have occurred before the date of acceptance of this Agreement by the Court, but in developing such understanding the Monitor is to rely to the extent possible on available information and documents provided by the Company, and it is not intended that the Monitor will conduct his own inquiry into those historical events. In developing each work plan and in carrying out the reviews pursuant to such plans, the Monitor is encouraged to coordinate with Company personnel including auditors and compliance personnel and, to the extent the Monitor deems appropriate, the Monitor may rely on the Company processes, on the results of studies, reviews, audits and analyses conducted by or on behalf of the Company and on sampling and testing methodologies. The Monitor is not expected to conduct a comprehensive review of all business lines, all business activities or all markets. Any disputes between the Company and the Monitor with respect to the work plan shall be decided by the Department in its sole discretion.

4. The initial review shall commence no later than ninety (90) calendar days from the date of the engagement of the Monitor (unless otherwise agreed by the Company, the Monitor and the Department), and the Monitor shall issue a written report within ninety (90) calendar days of initiating the initial review, setting forth the Monitor's assessment and making recommendations reasonably designed to improve the effectiveness of the Company's anti-fraud

and anti-money laundering programs for ensuring compliance with the Bank Secrecy Act. The Monitor is encouraged to consult with the Company concerning his findings and recommendations on an ongoing basis, and to consider and reflect the Company's comments and input to the extent the Monitor deems appropriate. The Monitor need not in its initial or subsequent reports recite or describe comprehensively the Company's history or compliance policies, procedures and practices, but rather may focus on those areas with respect to which the Monitor wishes to make recommendations for improvement or which the Monitor otherwise concludes merit particular attention. The Monitor shall provide the report to the Board of Directors of the Company and contemporaneously transmit copies to the Chief of the Asset Forfeiture and Money Laundering Section, Criminal Division, U.S. Department of Justice, at 1400 New York Avenue N.W., Bond Building, Washington, DC 20530 and the United States Attorney for the Middle District of Pennsylvania, 228 Walnut Street, Suite 220, Harrisburg, PA 17108. After consultation with the Company, the Monitor may extend the time period for issuance of the report for up to thirty (30) calendar days with prior written approval of the Department.

5. Within ninety (90) calendar days after receiving the Monitor's report, the Company shall adopt all recommendations in the report; provided, however, that within thirty (30) calendar days after receiving the report, the Company shall notify the Monitor and the Department in writing of any recommendations that the Company considers unduly burdensome, inconsistent with local or other applicable law or regulation, impractical, costly or otherwise inadvisable. With respect to any recommendation that the Company considers unduly burdensome, inconsistent with local or other applicable law or regulation, impractical, costly or otherwise inadvisable, the Company need not adopt that recommendation within that time but

shall propose in writing an alternative policy, procedure or system designed to achieve the same objective or purpose. As to any recommendation on which the Company and the Monitor do not agree, such parties shall attempt in good faith to reach an agreement within thirty (30) calendar days after the Company serves the written notice. In the event the Company and the Monitor are unable to agree on an acceptable alternative proposal, the Company shall promptly consult with the Department, which will make a determination as to whether the Company should adopt the Monitor's recommendation or an alternative proposal, and the Company shall abide by that determination. Pending such determination, the Company shall not be required to implement any contested recommendation(s). With respect to any recommendation that the Monitor determines cannot reasonably be implemented within ninety (90) calendar days after receiving the report, the Monitor may extend the time period for implementation with prior written approval of the Department.

6. The Monitor shall undertake at least four (4) follow-up reviews to carry out the Mandate. Within ninety days (90) calendar days of initiating each follow-up review, the Monitor shall: (a) complete the review; (b) certify whether the compliance program of the Company, including its policies and procedures, is reasonably designed and implemented to detect and prevent fraud and money laundering and to comply with the Bank Secrecy Act; and (c) report on the Monitor's findings in the same fashion as set forth in paragraph 4 with respect to the initial review. The first follow-up review shall commence one year after the initial review commenced. The second follow-up review shall commence one year after the first follow-up review commenced. The third follow-up review shall commence one year after the second follow-up review commenced. The fourth follow-up review shall commence one year after the third follow-up review commenced. After consultation with the Company, the Monitor may extend

the time period for these follow-up reviews for up to sixty (60) calendar days with prior written approval of the Department.

7. In undertaking the assessments and reviews described in Paragraphs 3 through 6 of this Agreement, the Monitor shall formulate conclusions based on, among other things: (a) inspection of relevant documents, including the Company's current anti-fraud and anti-money laundering policies and procedures; (b) on-site observation of selected systems and procedures of the Company at sample sites, including internal controls and record-keeping and internal audit procedures; (c) meetings with, and interviews of, relevant employees, officers, directors and other persons at mutually convenient times and places; and (d) analyses, studies and testing of the Company's compliance program with respect to the anti-fraud and anti-money laundering programs.

8. Should the Monitor, during the course of his engagement, discover that questionable or corrupt activity involving fraud-induced money transfers, money laundering or the Company's anti-money laundering program either (a) after the date on which this Agreement or (b) that have not been adequately dealt with by the Company (collectively "improper activities"), the Monitor shall promptly report such improper activities to the Company's General Counsel or Compliance and Ethics Committee for further action. If the Monitor believes that any improper activity or activities may constitute a significant violation of law, the Monitor should also report such improper activity to the Department. The Monitor should disclose improper activities in his discretion directly to the Department, and not to the General Counsel or Compliance and Ethics Committee, only if the Monitor believes that disclosure to the General Counsel or the Compliance and Ethics Committee would be inappropriate under the circumstances, and in such case should disclose the improper activities to the General Counsel or

the Compliance and Ethics Committee of the Company as promptly and completely as the Monitor deems appropriate under the circumstances. The Monitor shall address in his reports the appropriateness of the Company's response to all improper activities, whether previously disclosed to the Department or not. Further, in the event that the Company, or any entity or person working directly or indirectly within the Company, refuses to provide information necessary for the performance of the Monitor's responsibilities, if the Monitor believes that such refusal is without just cause the Monitor shall disclose that fact to the Department. The Company shall not take any action to retaliate against the Monitor for any such disclosures or for any other reason. The Monitor may report any criminal or regulatory violations by the Company or any other entity discovered in the course of performing his duties, in the same manner as described above.

9. The Monitor shall meet with the Department within thirty (30) days after providing each report to the Department to discuss the report. The reports will likely include proprietary, financial, confidential, and competitive business information. Moreover, public disclosure of the reports could discourage cooperation, impede pending or potential government investigations and thus undermine the objectives of the Monitorship. For these reasons, among others, the reports and the contents thereof are intended to remain and shall remain non-public, except as otherwise agreed to by the parties in writing, or except to the extent that the Department determines in its sole discretion that disclosure would be in furtherance of the Department's discharge of its duties and responsibilities or is otherwise required by law.

10. At least annually, and more frequently if appropriate, representatives from the Company and the Department will meet together to discuss the Monitorship and any suggestions,

comments or improvements the Company may wish to discuss with or propose to the Department.